IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 1, 2, 5, 6, 8, 9, 11, 12, 14, and 20 and CANCEL claims 3, 4, 7, 10, 13, and 15-19 in accordance with the following:

1. (Currently Amended) A file security management method, comprising:

obtaining a position in which a file can be opened as current position information from a position detecting device or as position information from an input device, and obtaining data indicating a number of significant digits of the position information used for encryption or decryption of the file from the input device,

encrypting ~~a~~ the file by using, as a key, data having high-order digits corresponding to the number of significant digits of the position information obtained from the position information and the data indicating the number of significant digits;

further generating a first digest which is data resulting from a hash operation performed on the encrypted file, and generating public key encryption data by encrypting, using a public key, the data indicating the number of significant digits, the file encrypted using the position information as a key, and the first digest; and

generating a second digest by performing a hash operation on the generated public key encryption data, and generating data to be provided by adding the second digest to the public key encryption data ~~which specifies a position in which the file can be opened~~;

~~saving the encrypted file;~~

~~decrypting the file by using, as a key, position information which is detected by a position detecting device; and~~

~~displaying the decrypted file~~.

2. (Currently Amended) ~~The file security management method according to claim 1, wherein~~

~~a selection is made from among a plurality of preregistered positions when position information in which the file can be decrypted is selected~~.

A file security management method, comprising:

obtaining data to be provided having public key data which is generated by encrypting, using a public key, data indicating a number of significant digits of position information, a file encrypted using data corresponding to the number of significant digits of the position information, and a first digest obtained by performing a hash operation to the encrypted file, and a second digest obtained by performing a hash operation to the public key encryption data; and generating the data to be provided by adding the second digest to the public key encryption data;

generating a digest by performing a hash operation to the public key encryption data included in the data to be provided, and determining whether the generated digest matches the second digest included in the data to be provided;

decrypting, when the generated digest and the second digest matches, the public key encryption data using a secret key corresponding to the public key, and obtaining the data indicating the number of significant digits of the position information, the file encrypted using the position information and the first digest;

generating a digest by performing a hash operation to the obtained encrypted file, and determining whether the generated digest matches the obtained first digest; and

obtaining, when the generated digest and the first digest matches, current position information from a position detecting device, and performing decryption process of the obtained encrypted file using data having high-order digits corresponding to the number of significant digits of the current position information as a key.

3. (Cancelled)

4. (Cancelled)

5. (Currently Amended) A file security management apparatus, comprising:

an acquisition unit for obtaining a position in which a file can be opened as current position information from a position detecting device or as position information from an input device, and obtaining data indicating a number of significant digits of the position information used for encryption or decryption of the file from the input device;

an encrypting unit encrypting ~~a~~ the file by using, as a key, ~~position information which specifies a position in which the file can be opened;~~

~~a saving unit saving the encrypted file;~~

~~a decrypting unit decrypting the file by using, as a key, position information which is detected by a position detecting device; and~~

~~a displaying unit displaying the file decrypted by said decrypting unit~~ data having high-order digits corresponding to the significant number of digits of the position information obtained the position information and the data indicating the number of significant digits;

further generating a first digest which is data resulting from a hash operation performed on the encrypted file, and generating public key encryption data by encrypting, using a public key, the data indicating the number of significant digits, the file encrypted using the position information as a key, and the first digest; and

data to be provided to the generation unit generating a second digest by performing a hash operation on the generated public key encryption data, and generating data to be provided by adding the second digest to the public key encryption data.

6. (Currently Amended) A file security management apparatus, comprising:

a first acquisition unit for obtaining data to be provided having public key data which is generated by encrypting, using a public key, data indicating number of significant digits of position information, a file encrypted using data corresponding to the number of significant digits of the position information, and a first digest obtained by performing a hash operation to the encrypted file, and a second digest which is obtained by performing a hash operation to the public key encryption data; and generating the data to be provided by adding the second digest to the public key encryption data;

a first determination unit for generating a digest by performing a hash operation to the public key encryption data included in the data to be provided, and determining whether the generated digest matches the second digest included in the data to be provided;

a second acquisition unit for decrypting, when the generated digest and the second digest matches, the public key encryption data using a secret key corresponding to the public key, and obtaining the data indicating the number of significant digits of the position information, the file encrypted using the position information, and the first digest;

a second determination unit for generating a digest by performing a hash operation to the obtained encrypted file, and determining whether the generated digest matches the obtained first digest; and

a decryption unit for obtaining, when the generated digest and the first digest matches, current position information from a position detecting device, and performing

decryption process of the obtained encrypted file using data having high-order digits corresponding to the number of significant digits of the current position information as a key

~~A file security management method,~~

~~comprising:~~

~~encrypting a file by using, as a key, position information which specifies a position in which the file can be opened; and~~

~~saving the encrypted file~~.

7. (Cancelled)

8. (Currently Amended) A computer-readable storage medium on which a file security management program is recorded, the program comprising:

obtaining a position in which a file can be opened as current position information from a position detecting device or as position information from an input device, and obtaining data indicating a number of significant digits of the position information used for encryption or decryption of the file from the input device,

encrypting the file by using, as a key, data having high-order digits corresponding to the number of significant digits of the position information obtained from the position information and the data indicating the number of the significant digits;

further generating a first digest which is data resulting from a hash operation performed on the encrypted file, and generating public key encryption data by encrypting, using a public key, the data indicating the number of significant digits, the file encrypted using the position information as a key, and the first digest; and

generating a second digest by performing a hash operation on the generated public key encryption data, and generating data to be provided by adding the second digest to the public key encryption data ~~A file security management method,~~

~~comprising:~~

~~encrypting data by using position information which specifies a position in which the data can be used; and~~

~~transmitting the encrypted data, or saving the encrypted data onto a computer-readable storage medium~~.

9. (Currently Amended) A computer-readable storage medium on which a file security management program is recorded, the program comprising:

obtaining data to be provided having public key data which is generated by encrypting, using a public key, data indicating a number of significant digits of position information, a file encrypted using data corresponding to the number of significant digits of the position information, and a first digest obtained by performing a hash operation to be the encrypted file, and a second digest which is obtained by performing a hash operation to the public key encryption data; and generating the data to be provided by adding the second digest to the public key encryption data;

generating a digest by performing a hash operation to the public key encryption data included in the data to be provided, and determining whether the generated digest matches the second digest included in the data to be provided;

decrypting, when the generated digest and the second digest matches, the public key encryption data using a secret key corresponding the public key, and obtaining the data indicating the number of significant digits of the position information, the file encrypted using the position information and the first digest;

generating a digest by performing a hash operation to the obtained encrypted file and determining whether the generated digest matches the obtained first digest;

obtaining, when the generated digest and the first digest matches, current position information from a position detecting device, and performing a decryption process of the obtained encrypted file using data having high-order digits corresponding the number of significant digits of the current position information as a key

~~The file security management method~~

~~according to claim 8, wherein a limitation is imposed on a position range in which a file can be opened by changing a data length of position information used as an encryption key~~.

10. (Cancelled)

11. (Currently Amended) The computer-readable storage medium of claim 8, A ~~program security management method, comprising:~~

~~encrypting a program with position information which specifies a position in which the program can be used; and~~

~~transmitting the program encrypted with the position information, or saving the encrypted program onto a computer-readable storage medium~~ wherein said encrypting includes encrypting the program with the position information which specifies a position in which the program can be used.

12. (Currently Amended) The computer-readable medium of claim 11, wherein said encrypting includes encrypting the program with the position information and a license key given to a user ~~program security management method~~

~~according to claim 11, wherein the program is encrypted with the position information, and a license key given to a user~~.

13. (Cancelled)

14. (Currently Amended) ~~A program security management method~~The computer-readable medium of claim 9, comprising:

~~encrypting a program with position information which specifies a position in which the program can be used;~~

~~transmitting the program encrypted with the position information, and a license key given to a user;~~

~~receiving, by the user, the encrypted program and the license key; and~~

~~decrypting the encrypted program with position information which is detected by a position detecting device, and the license key~~receiving a program encrypted using position information and a license key, and

decrypting the encrypted program with position information which is detected by a position detecting device and the license key.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Currently Amended) ~~A computer-readable storage medium on which is recorded a program for reading map data from a storage medium on which is recorded map data~~

~~encrypted with position information which specifies a position in which the map data can be used, the program comprising~~

~~allowing the map data to be decrypted only if position information detected by a position detecting device and the position information used to encrypt the map data match~~The computer-readable storage medium according to claim 8, on which is recorded a program for reading map data from a storage medium on which is recorded map data encrypted with position information which specifies a position in which the map data can be used, the program including allowing the map data to be decrypted only if position information detected by a position detecting device and the position information used to encrypt the map data match.